



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/452,329 | 11/30/1999 | GARY L. GRAUNKE | 42390.P7947 | 1161 |

7590

09/29/2003

ALOYSIUS T C AU YEUNG
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
12400 WILSHIRE
7TH FLOOR
LOS ANGELES, CA 90025

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 09/29/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/452,329

Applicant(s)

GRAUNKE ET AL.

Examiner

Christian La Forgia

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 March 2000.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 November 1999 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☒ Other: PTO-1533.

DETAILED ACTION

1. Claims 1 through 21 are presented for examination.

Drawings

2. The informal drawings filed in this application are acceptable for examination purposes.

When the application is allowed, applicant will be required to submit new formal drawings.

3. The Patent and Trademark Office no longer makes drawing changes. See 1017 O.G. 4.

It is applicant's responsibility to ensure that the drawings are corrected. Corrections must be made in accordance with the instructions below.

INFORMATION ON HOW TO EFFECT DRAWING CHANGES

Replacement Drawing Sheets

Drawing changes must be made by presenting replacement figures which incorporate the desired changes and which comply with 37 CFR 1.84. An explanation of the changes made must be presented either in the drawing amendments, or remarks, section of the amendment. Any replacement drawing sheet must be identified in the top margin as "Replacement Sheet" and include all of the figures appearing on the immediate prior version of the sheet, even though only one figure may be amended. The figure or figure number of the amended drawing(s) must not be labeled as "amended." If the changes to the drawing figure(s) are not accepted by the examiner, applicant will be notified of any required corrective action in the next Office action. No further drawing submission will be required, unless applicant is notified.

Identifying indicia, if provided, should include the title of the invention, inventor's name, and application number, or docket number (if any) if an application number has not been assigned to the application. If this information is provided, it must be placed on the front of each sheet and centered within the top margin.

Annotated Drawing Sheets

A marked-up copy of any amended drawing figure, including annotations indicating the changes made, may be submitted or required by the examiner. The annotated drawing sheets must be clearly labeled as "Annotated Marked-up Drawings" and accompany the replacement sheets.

Timing of Corrections

Art Unit: 2131

Applicant is required to submit acceptable corrected drawings within the time period set in the Office action. See 37 CFR 1.85(a). Failure to take corrective action within the set period will result in ABANDONMENT of the application.

If corrected drawings are required in a Notice of Allowability (PTOL-37), the new drawings MUST be filed within the THREE MONTH shortened statutory period set for reply in the "Notice of Allowability." Extensions of time may NOT be obtained under the provisions of 37 CFR 1.136 for filing the corrected drawings after the mailing of a Notice of Allowability.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. As per claims 1 through 9, merely claimed as a stream cipher representing a data string *per se*, that is, descriptions or expressions of such a string and that is, descriptive material *per se*, non-functional descriptive material, and is not statutory because it is not a physical "thing" nor a statutory process, as there are not "acts" being performed. Such claimed data strings do not define any structural and functional interrelationships between the data string and other claimed aspects of the invention which permit the computer program's functionality to be realized. Since a data string is merely a series of bits capable of being executed by a computer, the data string itself is not a process, without the device to generate a stream cipher needed to realize the data string's functionality. In contrast, a claimed device for generating a stream cipher defines structural and functional interrelationships between the data string and the medium which permit the data string's functionality to be realized, and is thus statutory. **Warmerdam**, 33 F.3d at 1361, 31 USPQ2d at 1760. **In re Sarkar**, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978). See MPEP § 2106(IV)(B)(1)(a).

Art Unit: 2131

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1 through 3, 7 through 13, and 17 through 21 are rejected under 35 U.S.C. 102(b) as being anticipated by United States Patent No. 5,703,952 to Taylor, hereinafter Taylor.

8. As per claim 1, Taylor teaches a stream cipher comprising:

a first and a second data bit generator to generate in parallel a first and a second stream of data bits (Figures 1 [blocks 8], 2 [blocks 8], 3 [blocks 8]; column 2, lines 39-52; column 4, lines 2-32); and

a combiner function coupled to the first and second data bit generators, having a shuffle unit including a storage structure, to generate a pseudo random sequence by modifying the first stream of data bits with at least a stochastic stream of past values of the first stream of data bits generated by using the second stream of data bits to stochastically operate the storage structure of the shuffle unit to memorize and reproduce past values of the first stream (Figure 2 [blocks 10, 12, 26], 3 [blocks 10, 12, 17, 26]; column 2, line 38 to column 3, line 3; column 4, lines 26-64; column 6, lines 12-23; column 11, lines 17-26; column 12, lines 30-67).

9. Regarding claims 2, 11, and 21, Taylor teaches wherein the combiner function generates the past values of the first stream of data bits by using the second stream of data bits to stochastically control writing of the first stream of data bits into storage locations of the storage structure, and at the same time, retrieving past written values from the storage locations being

Art Unit: 2131

written into (Figure 2 [blocks 10, 12, 26], 3 [blocks 10, 12, 17, 26]; column 6, lines 12-23; column 7, lines 42-48; column 11, lines 17-26; column 12, lines 30-67).

10. Regarding claims 3 and 12, Taylor teaches wherein at least one of the first and the second data bit generator comprises a linear feedback shift register (Figures 1 [blocks 8], 2 [blocks 8], 3 [blocks 8]; column 2, lines 39-52; column 3, lines 24-28; column 4, lines 2-32).

11. Regarding claims 7 and 17, Taylor teaches wherein the stream cipher further comprises a third data bit generator coupled to the combiner function to generate a third stream of data bits for the combiner function, and the combiner function is to further operate the storage structure to memorize and reproduce past values of the first stream using the third stream of data bits (Figures 2 and 3; column 10 line 66 to column 11, line 11; column 11, line 15 to column 12, line 21; column 12, line 30 to column 13, line 23).

12. With regards to claims 8 and 18, Taylor teaches wherein the stream cipher further comprises a fourth data bit generator coupled to the combiner function to generate a fourth stream of data bits for the combiner function, and the combiner function is to further operate the storage structure to memorize and reproduce past values of the first stream using the fourth stream of data bits (Figures 2 and 3; column 10 line 66 to column 11, line 11; column 11, line 15 to column 12, line 21; column 12, line 30 to column 13, line 23).

13. Regarding claims 9 and 19, Taylor teaches wherein the combiner function further comprises a XOR function coupled to the first bit data generator and the storage unit to generate

Art Unit: 2131

the pseudo random sequence by performing an XOR function on at least said first stream and its past values (column 11, lines 17-26).

14. As per claim 10, Taylor teaches a method comprising:

generating in parallel a first and a second stream of data bits (Figures 1 [blocks 8], 2 [blocks 8], 3 [blocks 8]; column 2, lines 39-52; column 4, lines 2-32);

stochastically generating a stream of past values of the first stream of data bits using the second stream of data bits (Figure 2 [blocks 10, 12, 26], 3 [blocks 10, 12, 17, 26]; column 2, line 38 to column 3, line 3; column 4, lines 26-64; column 6, lines 12-23; column 11, lines 17-26; column 12, lines 30-67); and

generating a pseudo random sequence by combining the first stream of data bits with at least the stochastically generated stream of past values of the first stream (Figure 2 [blocks 10, 12, 26], 3 [blocks 10, 12, 17, 26]; column 2, line 38 to column 3, line 3; column 4, lines 26-64; column 6, lines 12-23; column 11, lines 17-26; column 12, lines 30-67).

15. With regards to claim 13, Taylor teaches wherein the method further comprises initializing the first feedback shift register with a first plurality of key segments, and the second linear feedback shift register with a second plurality of key segments and at least one initial vector segment (column 2, line 53 to column 3, line 13).

16. As per claim 20, Taylor teaches an apparatus comprising:

Art Unit: 2131

first and second data bit generation means for generating in parallel a first and a second stream of data bits (Figures 1 [blocks 8], 2 [blocks 8], 3 [blocks 8]; column 2, lines 39-52; column 4, lines 2-32); and

combiner means coupled to the first and second data bit generation means, including shuffling means having storage means, for generating a pseudo random sequence, by combining the first stream of data bits with at least a stochastically generated stream of past values of the first stream of data bits generated by using the second streams of data bits to stochastically operate the storage means of the shuffle means to memorize and reproduce past values of the first stream (Figure 2 [blocks 10, 12, 26], 3 [blocks 10, 12, 17, 26]; column 2, line 38 to column 3, line 3; column 4, lines 26-64; column 6, lines 12-23; column 11, lines 17-26; column 12, lines 30-67).

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

18. Claims 4 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Taylor in lieu of obviousness.

19. Regarding claims 4 and 14, Taylor does not teach wherein the storage structure comprises a memory unit having a plurality of addressable memory locations, an input port coupled to the first data bit generator, an output port, at least one read address port and at least one write address port coupled to the second data bit generator.

Art Unit: 2131

20. Taylor teaches toward wherein the storage structure comprises a memory unit having a plurality of addressable memory locations, an input port coupled to the first data bit generator, an output port, at least one read address port and at least one write address port coupled to the second data bit generator (column 2, lines 39-52). It would have been obvious to one of ordinary skill in the art at the time the invention was made to place a memory unit at the output of first data bit generator and the input of the second data bit generator. One would be motivated to incorporate memory into the system of Taylor to ensure at least one sequence based on that of a previous value, thereby creating a method of two random sequences being generated.

21. Claims 5, 6, 15, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Taylor in view of United States Patent No. 6,069,954 to Moreau, hereinafter Moreau.

22. Regarding claims 5 and 15, Taylor does not teach wherein the combiner function comprises a 1 to n de-multiplexor having an input bit line coupled to said first data bit generator, n output bit lines coupled to the storage structure, and at least one control bit line coupled to said second data bit generator, where n is an integer greater than 1.

23. Moreau teaches wherein the combiner function comprises a 1 to n de-multiplexor having an input bit line coupled to said first data bit generator, n output bit lines coupled to the storage structure, and at least one control bit line coupled to said second data bit generator, where n is an integer greater than 1 (Figures 2, 3; column 7, line 52 to column 8, line 6). It would have been obvious to one ordinary skill in the art at the time the invention was made to include a de-multiplexor into the combiner function. One would be motivated to do so because the de-

Art Unit: 2131

multiplexor offers a simple and easier solution for dealing with more than two data bit generators. The combination is proper as both patents deal with similar encryption techniques.

24. Regarding claims 6 and 16, Taylor does not teach wherein the combiner function comprises an n to 1 multiplexor having n output bit lines coupled to said storage structure, an output bit line, and at least one control bit line coupled to said second data bit generator, where n is an integer greater than 1.

25. Moreau teaches wherein the combiner function comprises an n to 1 multiplexor having n output bit lines coupled to said storage structure, an output bit line, and at least one control bit line coupled to said second data bit generator, where n is an integer greater than 1 (Figures 2, 3; column 7, line 52 to column 8, line 6). It would have been obvious to one ordinary skill in the art at the time the invention was made to include a multiplexor into the combiner function. One would be motivated to do so because the multiplexor offers a simple and easier solution for dealing with more than two data bit generators. Additionally it provides for one more technique to ensure that a number is selected from the multitude of random data bit generators. The combination is proper as both patents deal with similar encryption techniques.

Conclusion

26. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

27. The following patents are cited to further show the state of the art with respect to stream ciphers, such as:

Art Unit: 2131

United States Patent No. 6,587,562 to Jansen et al., which is cited to show synchronous stream cipher.

United States Patent No. 6,351,539 to Djakovic, which is cited to show a cipher mixer with random number generator.

United States Patent No. 4,815,130 to Lee et al., which is cited to show a stream cipher system with feedback.

United States Patent No. 6,128,737 to Jakubowski et al., which is cited to show a method and apparatus for producing a message authentication code in a cipher block chaining operation by using linear combinations of an encryption key.

United States Patent No. 4,316,055 to Feistel, which is cited to show a stream cipher cryptographic system.

United States Patent No. 6,490,354 to Venkatesan et al., which is cited to show a lightweight word-oriented technique for generating a pseudo-random sequence for use in a key stream of a stream cipher.

28. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704. The examiner can normally be reached on Monday thru Thursday 7-5.

29. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

30. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Application/Control Number: 09/452,329

Page 11

Art Unit: 2131

Christian La Forgia
Patent Examiner
Art Unit 2131

clf



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100